Dominique Petersen, Sebastian Barchnicki, Norbert Pohlmann

Schutz- und Frühwarnsysteme für mobile Anwendungen

Angriffspotentiale, Schutzmechanismen und Forschungsaspekte für Smart Mobile Devices

Smart Mobile Devices (SMD) finden wegen ihrer unbegrenzten Konnektivität hohe Nutzerakzeptanz, sind aber auch – gerade deshalb - die Achillesferse der IT-Sicherheit. In diesem Beitrag werden die vielfältigen Angriffsvektoren und Schwachstellen von SMD's in unterschiedlichen Anwendungsumgebungen systematisiert und verfügbare Schutzmechanismen kritisch analysiert. Optimal kann mit diesen Mitteln nur ein Schutz vor bekannten Bedrohungen geleistet werden. Daher sind zusätzlich intelligente Systeme sinnvoll, mit denen unbekannte Bedrohungen und Angriffe erkannt werden könnten. Über einen solchen erfolgversprechenden Anomalieerkennungsansatz wird im Beitrag berichtet.

Dominique Petersen

ist wissenschaftlicher Mitarbeiter am Institut für Internet-Sicherheit der Westfälischen Hochschule in Gelsenkirchen undbet reut dort seit Januar 2007 den Bereich der Internet-Frühwarnsysteme als Projektleiter.
E-Mail: petersen@internet-sicherheit.de

Sebastian Barchnicki

ist studentischer Mitarbeiter am Institut für Internet-Sicherheit der Westfälischen Hochschule in Gelsenkirchen und dort im Bereich Internet-Frühwarnsysteme und Mobile-Security tätig.
E-Mail: barchnicki@internet-sicherheit.de

Norbert Pohlmann

Professor für Informationssicherheit und geschäftsführender Direktor des Instituts für Internet-Sicherheit an der Fachhochschule Gelsenkirchen sowie Vorstandsvorsitzender des TeleTrusT – Bundesverband IT-Sicherheit.

E-Mail: norbert.pohlmann@internet-sicherheit.de

1 Einleitung

Smart Mobile Devices (SMD) wie z.B. Smartphones sind klein, mobil und können fast überall genutzt werden. Auch der Begriff „Always-On" hat sich mittlerweile stark manifestiert, denn die Verbindung ins weltweite Datennetz ist heute nicht nur überall und jederzeit möglich, sondern auch permanent aktiv. Dem interessierten Nutzer stehen sehr große Bandbreiten für sehr wenig Geld zur Verfügung. Ist das Internet über Mobilfunk zu schmalbandig oder nicht verfügbar, kann und wird oft auf das meist deutlich schnellere WLAN in Verbindung mit örtlichem Breitband ausgewichen, ganz egal ob Zuhause, im Unternehmen oder an öffentlichen Plätzen im In- und Ausland.

Die ständige Netzverfügbarkeit sorgt für eine rapide Entwicklung: Der Markt für SMDs wächst massiv, nicht nur im privaten, sondern auch besonders im Unternehmen als Nutzbringer für den täglichen Arbeitsablauf und mobile Geschäftsprozesse im Tagesgeschäft. Alleine im Bereich der Android-Plattform werden weltweit täglich 1,5 Millionen neue SMDs aktiviert (Stand: 04/2013), Tendenz steigend. Hinzu kommen natürlich zahlreiche andere Hersteller und ihre Plattformen, die dabei noch nicht berücksichtigt worden sind. Die SMDs feiern also einen regelrechten Siegeszug und nehmen in allen Bereichen des Lebens immer mehr Raum ein. Es sind verschiedene Gründe, die den Benutzer dazu motivieren, ein solches SMDs zu besitzen: Es kann immer und überall genutzt werden, ist sehr hilfreich im Alltag und bei der Arbeit oder dient einfach auch nur als Statussymbol in goldener Ausführung.

Gleichzeitig gilt es eben diese mobilen Geräte auch in eine bestehende IT-Landschaft zu integrieren, ohne das Risiko durch Angriffe von außen zu erhöhen. Gerade SMDs werden zunehmend zur Zielscheibe für Angriffe mit Spionageabsichten oder

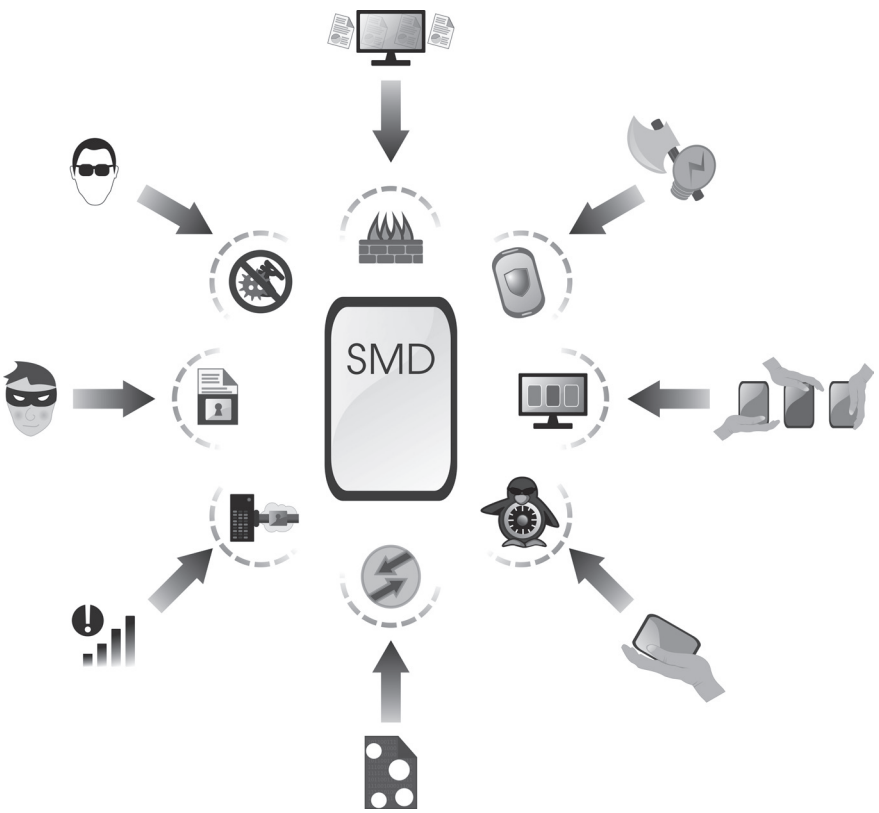
Identitätsdiebstahl, denn schließlich beinhalten SMDs zahlreiche Daten wie Fotos, Videos und Tonaufnahmen, Zugangsdaten, Nachrichten und viele andere sensible Daten. Hierbei können auch aufmerksame und versierte Nutzer in die Falle tappen: Menschen machen Fehler und Angreifer versuchen häufig eben aus dieser Tatsache einen Nutzen zu ziehen.

Durch die Integration von SMDs in die bestehende Infrastruktur eines Unternehmens entsteht ein neuer Angriffsvektor. Um das bestehende Sicherheitsniveau der Infrastruktur weiterhin zu gewährleisten, müssen sichere Konfigurationen der SMDs etabliert und deren Gewährleistung sichergestellt werden. Die Frage ist, ob sich mit bestehenden Mitteln und vorhanden Technologien diese Herausforderung lösen lässt oder ob die heutige Situation eine neue Denkweise und neue Lösungsansätze bedarf, um einen echten und vor allem sicheren Mehrwert zu bieten.

2 Gefahrenpotentiale

Die privaten Vorteile von mobilen Geräten, wie SMDs sind bestechend: Über die vielfältigen Kommunikationsschnittstellen (WLAN, UMST/LTE, Bluetooth, NFC, usw.) ist das Internet mit seinen zentralen Diensten stets und überall verfügbar. Die immer leistungsstärkeren mobilen Geräte sind einfach und schnell über Touchscreens zu bedienen. Weiterhin stellen diese Geräte viele und praktische Funktionen bereit: Sie sind Handy, Computer, Navigationssystem, MP3-Player/TV-Gerät, Medizin-/Gesundheitsgerät, Zugang zum Unternehmen - alles vereint in einem handlichen Gerät in Form eines ständigen Begleiters.

Abbildung 1 | Bedrohungen und Schutzmechanismen für ein Smart Mobile Device (SMD)



Die Anzahl der verfügbaren Apps ist riesig und wächst stetig an. Apps stehen unkompliziert und kostenlos oder zumindest preisgünstig zur Verfügung, und vor allem: Es gibt für jedes Problem mindestens ein Dutzend Apps, sodass auf einem SMD häufig viele verschiedene Programme installiert sind. So sind auf aktuellen SMDs im Auslieferungszustand bereits ca. 50 Apps vorinstalliert, und nicht selten erhöht sich diese Zahl durch die Installation des Nutzers weiterer Apps auf über 100. Mit „Location Based Services" kommen innovative Vor-Ort-Dienste für den Privatanwender hinzu. Erst durch die Installation von Apps und der Nutzung dieser Dienste wird solch ein SMD personalisiert und erfüllt die ganz persönlichen Anforderungen seines Besitzers. Gerade diese Personalisierung birgt aber weitere Risiken (siehe Abbildung 1).

3 Konkrete Angriffe auf SMDs

3.1 Software-Lücken

Ein hoher Verbreitungsgrad eines Produkts hat meist zur Folge, dass es in den Fokus krimineller Menschen rückt. Betriebssysteme und die darin enthaltenen Komponenten sind nie ganz perfekt und beinhalten immer Fehler. Mit genügend Aufwand und Ressourcen lässt sich in praktisch jeder Software Fehler und damit einen Angriffspunkt finden. Das können fehlerhafte Browser, E-Mail-Programme oder ein nicht fehlerfrei arbeitender Lock-Screen sein, der trotz PIN-Sperre den Zugriff auf das Telefon ermöglicht, wie in der Vergangenheit bereits mehrfach geschehen.

Diese Sicherheitsprobleme lassen sich nur durch die Pflege und Optimierung der Software seitens der Hersteller beheben. Wurde die Entwicklung einer Software jedoch eingestellt oder hat der Hersteller sich dazu entschlossen den Support zu beenden, bleiben die Nutzer mit den vorhanden Sicherheitslücken alleine, auch wenn das Gerät aus technischer Sicht nach wie vor noch lange nicht am Ende seines Lebenszyklus angekommen ist. Leider ist diese Praxis im Bereich von SMDs allgegenwärtig, da Hersteller für Weiterentwicklungen und Updates personelle Ressourcen zur Verfügung stellen müssen. Diese kosten Geld, aber durch die bereits einmalig verkauften Geräte können keine weiteren Einnahmen mehr generiert werden. Der Zyklus gestaltet sich wie folgt: In der Praxis wird dann zügig ein neues SMD vorgestellt, das ab Werk mit aktualisierter Software ausgeliefert wird.

3.2 Root-Exploits

Android besitzt, obwohl es aus der Linux-/Unixfamilie stammt, keine Benutzerverwaltung im klassischen Sinne. Der Anwender hat keine bestimme Identität auf dem SMD, sondern ist der einzige Benutzer und gleichzeitig der Besitzer. Prinzipiell arbeitet der Nutzer auf einem Android-Gerät mit eingeschränkten Rech-

ten. Da jede Anwendung jeweils nach verschiedenen spezifischen Rechten verlangt und während der Installation vom Anwender die Freigabe dieser erhalten hat, übernimmt ein virtueller Benutzer jeweils die Identität und Rechte einer einzelnen Anwendung. Im Prinzip legt die virtuelle Maschine also für jede laufende App einen eigenen Benutzer an.

Je mehr Rechte eine App bekommt, auf desto mehr Informationen oder Hardwarekomponente darf sie zugreifen. Das bedeutet auch, dass der Hersteller alle Daten, die sich auf dem SMD befinden, an seine Server übermitteln kann – egal wie kritisch diese Informationen sind. Besonders tückisch daran: Das alles kann passieren, ohne dass der Nutzer darüber informiert oder bei ihm nachfragt werden muss. Diese erzwungene Beschränkung hat aber auch Vorteile, da der Anwender – bewusst oder unbewusst – nur begrenzt Schäden an seiner Hard– und Software anrichten kann.

Es ist jedoch möglich, die vollen Rechte als Administrator auf einem SMD zu erlangen. Dieser Vorgang wird „rooten" genannt und hat weitreichende Konsequenzen. Denn ab diesem Zeitpunkt ist es nicht nur möglich, tief gehende Systemmanipulationen durchzuführen, sondern auch die Hardware über die spezifizierten Grenzen hinaus auszureizen und damit sogar zu beschädigen. Bei Apples iOS ist dies ebenfalls möglich (der sog. „Jailbreak"), genau wie auch beim Windows Phone von Microsoft. Solche Root-Exploits werden üblicherweise vom Anwender durchgeführt, um mehr Rechte auf dem SMD zu erhalten. Jedoch gab es in der Vergangenheit auch bereits Fälle, in denen Angreifer durch geschickte Manipulationen SMDs von unwissenden Anwendern „gerootet" haben.

Root-Exploits stellen ein beträchtliches Risiko für die Sicherheit dar. Ein Root-Exploit ist eine Schwachstelle im Betriebssystem, die es einem Angreifer erlaubt, Administratorrechte (sog. Root-Rechte) auf dem SMD zu erhalten. Standardmäßig gestattet bspw. Android die Arbeit nur mit eingeschränkten Rechten und verhindert so den Zugriff auf kritische Systembereiche wie beispielsweise den Bootloader oder die System- und App-Datenbanken. Durch einen Root-Exploit kann im Fall von Android praktisch das komplette Sicherheitssystem umgangen werden.

Die Schwachstellen können durch einen Fehler in einer Kernkomponente von Android wie z.B. Webkit oder durch die Anpassung des Betriebssystems durch den Hersteller entstehen. Ein bekanntes Beispiel hierfür ist der Exynos-Exploit, der diverse SMD verschiedener Hersteller betraf.

Es gibt zwei Arten von Root-Exploits auf einem Gerät: Permanent und flüchtig. Im letzteren Fall wird einfach nur eine Command-Shell mit Root-Rechten erzeugt, um einzelne Befehle abzusetzen. Wird die Shell beendet, verfallen die Root-Rechte. Permanente Root-Rechte werden erreicht, indem ein automatisches Rooten beim Start des Systems hinterlegt wird. Dieses wird meist in Form einer App realisiert und gibt der ausführenden Command-Shell oder App dauerhaft Root-Rechte. Während sich permanente Root-Rechte einfach erkennen lassen sind aktuelle Sicherheitslösungen nicht in der Lage, einen flüchtigen Root-Exploit zu erkennen, wenn dieser verwendet wird.

3.3 Diebstahl und Verlust

Ständig wechselnde und potentiell unsichere Umgebungen (Flughäfen, Bahnhöfen, Cafés) erhöhen die Wahrscheinlichkeit eines unabsichtlichen Verlustes oder des gezielten Diebstahls von Gerät, Daten oder Identität. Anders als der Computer auf dem Schreibtisch ist ein SMD sehr klein und immer dabei. Dadurch wird das Risiko eines Verlustes sehr groß: Laut einer Studie von Lookout Security aus dem Jahre 2008 gingen jeden Tag SMDs im Wert von 7.000.000 USD verloren. Bei einem Durchschnittspreis von etwa 400 USD sind das etwa 17.500 SMDs pro Tag. Aktuell wird diese Zahl nochmals deutlich darüber liegen. Besonders sicherheitskritisch: Im von Symantec im März 2012 durchgeführten „SMD Honey Stick Project" Experiment versuchten über 50% der Finder auf Firmendaten zuzugreifen, wenn sie die Möglichkeit dazu sahen. Im Detail wollten 57% der Finder Zugriff auf die Passwörter erlangen und 45% auf die geschäftlichen E-Mails. Neben dem unabsichtlichen Verlust eines SMDs kann auch ein konkurrierendes Unternehmen oder eine Institution einen Taschendieb mit dem Diebstahl des Geräts beauftragen, um so Wirtschaftsspionage zu betreiben, ohne einen aufwändigen Angriff auf hoch gesicherte Unternehmensserver durchzuführen zu müssen.

3.4 Öffentliche WLAN-Hotspots

Die Nutzung von öffentlichen, oft unverschlüsselten Drahtlosnetzwerken (WLANs/Hotspots) birgt eine Vielzahl an Gefahren: Zum einen kann ein Angreifer die unverschlüsselte Kommunikation des mobilen Geräts zum Netzwerk mitlesen, zum anderen ist nicht immer feststellbar, wem das fremde Netzwerk tatsächlich gehört. Da der Name eines solchen „Hotspots" frei wählbar ist, kann ein Angreifer einen bekannten Namen wie "Telekom" oder "BurgerKing" verwenden, um Seriosität vorzutäuschen. Verbindet sich das SMD mit dem Netzwerk, hat der Angreifer Zugriff auf sämtliche Daten, die über das Netz versendet werden, da die komplette Kommunikation über seinen Hotspot abgewickelt wird. Als Resultat können stark frequentierte Örtlichkeiten, wie beispielsweise Flughäfen, Cafés, Biergärten, etc., an denen Nutzer „nur mal eben E-Mails checken" wollen, zu einer wahren Fundgrube für sensible Informationen werden. Wird dann von den Apps keine Verschlüsselung gewählt, können nicht nur alle Daten mitgelesen werden. Der Angreifer kann darüber hinaus die Identität des Opfers annehmen, um weiteren Schaden zu verursachen. Als prominentes Beispiel gilt hier „Whatsapp", welches früher unverschlüsselt alle Daten übertragen hat und die Accounts sogar von Angreifern übernommen werden konnten.

3.5 Malware und Spionage-Apps

SMDs sind ab Werk mit einem Betriebssystem ausgestattet, welches die wichtigsten Grundfunktionen wie Telefonieren, SMS und E-Mails ermöglicht sowie einen Browser und weitere Apps bietet, die die Kernfunktionen des Geräts erweitern. Der Benutzer kann jedoch weitere Apps installieren, um den Funktionsumfang seines SMDs zu vergrößern und das Gerät zu personalisieren. Allein der App-Store von Google (Play Store) bietet derzeit über eine Millionen Apps an, die im Monat millionenfach heruntergeladen werden. Mitte 2013 zählte alleine Google Play über 50 Milliarden Downloads. Zudem gibt es noch alternative Quellen für Apps, wie den Amazon App Store oder das Android Pit App Center.

Vor dem Herunterladen einer App aus dem „Play Store" muss der Nutzer entscheiden, ob er der App den Zugriff auf weitere Daten wie Kontakte, E-Mails, Fotos, Anmeldedaten oder Informationen, die das Gerät und die SIM-Karte eindeutig identifizieren,

erlaubt. Dies ist problematisch, da die Nutzer nicht über die Weiterverarbeitung der gesammelten Daten informiert werden und sie keinerlei Kontrolle darüber haben, welche Daten wie oft abgerufen, übertragen und verarbeitet werden. Des Weiteren ist der Trend „Masse statt Klasse" in den verschiedenen App-Stores zu erkennen: Anbieter von Apps genehmigen sich lieber etwas mehr Rechte auf dem SMD als für die Funktion der angebotenen App eigentlich notwendig wäre. Dieser Trend steigert die Wahrscheinlichkeit, dass fehlerhafte oder aus sicherheitstechnischer Sicht bedenkliche Apps zum Download angeboten werden. Auch kann es passieren, dass trojanische Pferde (also Apps, die vorgeben einen nützlichen Zweck zu erfüllen, aber in Wirklichkeit Schadroutinen enthalten) im App-Store auftauchen. Gerade auf Android, wo Apps auch außerhalb des Play-Stores bezogen werden können („Sideloading"), können die Kontrollen von Google umgangen und Malware eingeschleust werden.

3.6 Datenaustausch mit dem Internet

Praktisch alle Apps, die auf einem SMD ausgeführt werden, kommunizieren mit dem Internet. Hierbei handelt es sich in erster Linie um gewollten Netzwerkverkehr, wie Updates, Werbeeinblendungen oder E-Mail-Kommunikation. Hat sich Malware auf dem System eingenistet, lädt diese üblicherweise auch Daten und ausgespähte Informationen ins Internet zu dem Angreifer. Für einen normalen Anwender eines SMDs ist ohne Hilfsmittel nicht ersichtlich, welche Apps und Dienste auf dem Gerät gerade wirklich laufen und welche Daten wohin übertragen werden. Im Worst-Case kann eine Malware auf einem SMD auch ein Einfallstor öffnen, über das sich der Angreifer auf das System einklinken und die volle Kontrolle übernehmen kann.

3.7 BYOD und Mischung Privat-/Unternehmensnutzung

SMDs sind auch aus den Unternehmen nicht mehr wegzudenken. Sie bieten Organisationen die Möglichkeit, bestehende Geschäftsprozesse zu optimieren oder durch die Mobilität der Mitarbeiter sogar neue Geschäftsfelder zu etablieren. Neben den neuen Chancen treten aber auch neue Risiken bei der Integration von SMDs in die Organisationsinfrastruktur auf: Die Geräte befinden sich meist außerhalb des überschaubaren und kontrollierbaren Organisationsumfelds und somit auch außerhalb der Sicherheitseinrichtungen der Organisation. Dies stellt eine nicht zu unterschätzende Gefahr dar, da SMDs fast die gleichen Möglichkeiten wie ein Computer bieten. Erschwerend kommt der Trend von BYOD (Bring Your Own Device) hinzu: Der Nutzer möchte ein SMD für alles haben, und benutzt dieses sowohl für berufliche als auch private Angelegenheiten. Somit können privat installierte Apps leicht auf sensible Unternehmensinformationen und sicherheitsrelevante Dienste zugreifen. Speziell die Integration in ein existierendes Organisationsnetzwerk und die Anbindung an bestehende Infrastrukturen verdienen unter dem Aspekt der Informationssicherheit besondere Beachtung: Sind Betriebssystem und Anwendungen auf dem aktuellsten Stand? Ist das mobile Gerät kompromittiert und stellt eine Gefahr für die Organisation dar? In welcher Art und Weise sind sensible Daten auf den mobilen Geräten gespeichert? Diese und noch weitere, sicherheitsrelevante Fragen müssen eindeutig beantwortet werden, damit die Integration von SMDs das bestehende Sicherheitsniveau einer Organisation nicht senkt und das Unternehmen konkret gefährdet.

3.8 Weitere Angriffsmöglichkeiten

Hinzu kommen weitere Angriffsvektoren, die auf den ersten Blick nicht einfach erkannt werden können. Auf vielen Werbetafeln, Wänden, im TV oder der Zeitung begegnen dem Benutzer immer häufiger QR Codes. Diese Grafiken sind codierte Informationen und können mit einem „Scanner" über die eingebaute Kamera eingelesen werden. Solch ein QR-Code kann bis ca. 3.000 Zeichen enthalten. Dies kann ein beliebiger Text sein, eine Internetadresse oder aber je nach SMD auch direkte Steuerinformationen, um bestimmte Aktionen im Gerät auszulösen. Im schlimmsten Fall leiten die hinter dem QR-Code hinterlegten Links auf eine infizierte Webseite, führen eine sofortige und irreversible Systemlöschung aller gespeicherter Daten durch oder sorgen durch wiederkehrende absichtliche Eingabe einer falscher PIN und anschließender PUK für die Sperrung und dem „Tod" der verwendeten SIM-Karte. Letzteres war vor einiger Zeit auf vielen Android-Geräten möglich. Es geht aber noch deutlich einfacher: So wurden in der Vergangenheit auf Wänden und Plakaten die originalen QR-Codes von Unbekannten unauffällig überklebt und der Inhalt so gegen Schadcode oder Fehlinformationen ausgetauscht.

4 Aktuelle Schutzmechanismen

4.1 Updateverhalten der Hersteller

Abhängig von der verwendeten Plattform bieten Hersteller eine breite Palette an verschiedensten Geräten und Softwareausstattungen mit diversen Erweiterungen und eigenen Zusätzen wie Oberflächen und Software-Paketen an. Ein Android System sieht und bedient sich auf einem SMD von Samsung anders als von HTC respektive LG. Dies liegt an sehr tiefgreifenden Modifikationen und Erweiterungen des originalen Betriebssystems durch weitere Treiber und Software.

Leider bringt Diversität auch große Probleme mit sich: Die Hersteller heben ihre Anpassungen in Verbindung mit der Auswahl an verschiedensten Geräteklassen gerne als Alleinstellungsmerkmale gegenüber der Konkurrenz heraus, allerdings ergeben sich daraus gravierende Nachteile: Neue Android-Versionen müssen nach der Erstveröffentlichung durch Google jedes Mal aufs Neue durch jeden Hersteller für sich und das spezielle SMDs aufwändig angepasst werden, was manchmal Monate dauert oder von vorne herein gänzlich verworfen wird aufgrund der daraus resultierenden hohen Kosten und dem Aufwand, der dem Hersteller keinen zusätzlichen Gewinn bringt. Diese Praxis sorgt leider für eine sehr hohe Fragmentierung auf dem Markt: Es gibt sehr viele Geräte mit noch mehr verschiedenen Android-Versionen, ganz egal ob gravierende Sicherheitslücken gefunden wurden oder sich Fehler eingeschlichen haben. Diese werden dann zum Nachteil der Nutzer und Entwickler ab diesem Zeitpunkt nicht mehr behoben. Die Hersteller sehen es lieber, „neue" SMDs absetzen zu können, welche aktuellere Software und Modifikationen ohne alte Sicherheitslücken beinhalten. Wir können an die Hersteller nur wiederholt appellieren, diese Praxis im Hinblick auf den Kunden und zur Reduktion der Gefahren zu überdenken und die Geräte für eine gewisse garantierte Zeit voll zu unterstützen. Hierdurch würden sehr viele Angriffsmöglichkeiten eliminiert werden können und SMDs würden im ökologischen Sinne auch längere Zeit Verwendung finden können. Es gibt aber auch Hersteller, die eine

kleine und sehr einheitliche Landschaft aus Hardware und Software anbieten, wie z.B. Apple mit iOS. Durch eine monotones Angebot und Einschränkung der Nutzer in einem hohen Maße wird hier versucht, Bedrohungen und der einfachen Auslieferung von Updates mit einer maximalen Reichweite Herr zu werden.

4.2 Vollverschlüsselung

Heutige SMDs bieten die Möglichkeit der Vollverschlüsselung, um bei einem Verlust des Gerätes die Einsicht von Daten gegenüber Dritten zu verhindern. So ist es möglich, den Inhalt des Gerätes und sogar die Daten auf der zusätzlich eingesetzten Speicherkarte zu verschlüsseln. Die Sicherheit hängt hierbei natürlich an der Komplexität des gewählten Passworts im Entsperrbildschirm ab. Ist dieses leicht zu erraten oder ein simpler Code, ist die vermeintlich „starke Verschlüsselung" hinfällig und leicht zu entschlüsseln.

4.3 VPN (Virtual Private Network)

Die Nutzung von öffentichen WLAN-Hotspots ist häufig nicht ungefährlich. Selbst scheinbar bekannte WLAN-Namen können mit ein wenig technischem Wissen gefälscht und Daten mitgelesen werden. Dies bedeutet, dass der Angreifer beinahe die gesamte Kommunikation mitschneiden und auswerten kann, sofern sie nicht von Beginn an verschlüsselt wird. Ist dessen Nutzung dennoch zwingend erforderlich, aber die Vertrauenswürdigkeit des verwendeten Hotspots kann nicht eingeschätzt und das WLAN muss risikofrei verwendet werden, gibt es als Schutzmechanismus die Möglichkeit, eine gesicherte Verbindung mittels eines VPN (Virtual Private Network) zu verwenden. Mittels eines VPN-Tunnels wird vor der eigentlichen Nutzung eines Hotspots eine gesicherte Verbindung zu einem vertrauenswürdigen Server im Internet aufgebaut, der dann den eigentlichen Zugriffspunkt auf die Daten im Internet darstellt. Die Kommunikation zu diesem Server wird komplett verschlüsselt und lässt sich nicht ohne weiteres ausspähen, weder durch neugierige Angreifer noch durch den Hotspotbetreiber selbst. Zusätzlich kann der VPN-Anbieter den Tunnel selbst ebenfalls mit zusätzlichen Sicherheitsfeatures ausstatten, wie Intrusion-Detection-Systeme und Anti-Viren-Lösungen. Ein Beispiel für so einen „Managed Secure VPN-Dienst"-Anbieter ist die Firma Secucloud.

4.4 Antivirus to go

Es existieren über 1 Millionen Apps im Google Play (Store), und aufgrund dieser Masse steigt natürlich auch das Risiko, dass in den einen oder anderen Apps Schädlinge oder Malware enthalten sind. Zwar führt Google heuristische Kontrollen der Inhalte durch und behält sich das Recht vor, im Fall einer nachträglichen Malwareklassifikation entsprechende Apps aus der Ferne auf den SMDs wieder zu deinstallieren, allerdings ist dann der Schaden oft schon entstanden. Zudem ist die Installation aus Drittanbieter App-Stores oder anderen unbekannten Quellen möglich, die von Google's Schutzmechanismen nicht berücksichtigt werden können.

Android hat eine sichere Architektur und bietet grundsätzlich einen sehr hohen Schutz. Aus einer genaueren Betrachtung der Sicherheitsbarrieren (Sandboxing, eingeschränkte Rechte) lässt sich ableiten, dass der Einsatz einer Antiviren-Software eigentlich nicht unbedingt notwendig und sinnvoll ist. Das Sandboxing hält schädliche Apps davon ab, sich im System auszubreiten und alle kritischen Bereiche zu infizieren. Zum einen bieten die aktuellen Sicherheits-Apps bei weitem keine sehr guten Erkennungsraten (weit unter 95%), und zum anderen verhindert eben diese Architektur die Einsicht in alle notwendigen Bereiche des Betriebssystems, um einen effektiven Schutz gewährleisten zu können. Zusätzlich verlangt solch ein Antiviren-Programm natürlich der Hardware einiges ab und sorgt für eine höhere Belastung des Systems und damit kürzere Akkulaufzeit. Für Apples iPhone gibt es im iTunes-Store keine Antivirus-Apps, da diese scheinbar erst gar nicht von Apple zugelassen werden. Apple möchte dem Problem mit eigenen Kontrollen der durch die Entwickler eingereichten Apps begegnen und erlaubt gar nicht erst Installation aus Drittquellen.

Wird auf einem SMD jedoch eine Antivirus-App genutzt, so hat dies auch eine weitere Kehrseite: Um annähernd effektiv handeln zu können, benötigt solch eine App umfangreiche Rechte und fordert auch den Zugriff auf personenbezogene Daten, Lesezeichen, Anrufe, SMS oder Kamera inkl. der Aufnahme von Bildern und Videos. Das entgegenzubringende Vertrauen durch den Anwender der sogar meist kostenlosen Apps muss sehr groß sein, und die Frage nach dem tatsächlichen verantwortungsvollen Umgang mit diesen eingeräumten Rechten und den persönlichen Daten bleibt natürlich offen.

4.5 Personal Firewall-Systeme (Paket-Filter)

SMDs sind der Dreh- und Angelpunkt hinsichtlich Datenaustausch mit dem Internet, also der Empfang und Versand von Informationen. Wie auf dem normalen Desktop-PC besteht auch auf dem SMD die Möglichkeit verschiedene Schutzvorkehrungen zu treffen, um die Kommunikation in alle Richtungen zu kontrollieren bzw. nach Belieben zu unterbinden. Hierfür bieten sich Paketfilter an, im Volksmund allgemein besser bekannt als Personal-Firewalls. Sie schützen vor ungewollt kommunizierenden Diensten und der Anwender kann mehr Kontrolle über den Datenfluss der Apps erlangen (mit Hinweis- und Abfragefenster, ob jeweilige Verbindung gewünscht). Für diese Filterung gibt es mittlerweile eine Auswahl an Apps, wie „DroidWall" oder „AFWall+".

4.6 SEAndroid

Gerade um private und berufliche Apps und Daten zu trennen, eignet sich das Konzept SEAndroid ideal. Abgeleitet von SELinux, was sich bei vielen Linux-Distributionen wie RedHat und Fedora bereits seit Jahren etabliert hat, ermöglicht SEAndroid eine Kapselung der zugreifbaren Daten für Programme/Apps. Hierbei wird für jedes Programm eine Policy erstellt, auf welche Daten und Ressourcen wie und in welcher Form zugegriffen werden darf. Da dieser Rechtemechanismus direkt im Kern des Betriebssystems umgesetzt wird, kommen Schadprogramme hierbei nicht aus der Isolation. Somit ist es möglich, private und berufliche Apps zu trennen. Bspw. kann so ein privat installiertes Spiel, welches normalerweise alle Daten auf dem SMD lesen darf, nur auf seine eigenen Dateien zugreifen, nicht aber auf die E-Mail-Korrespondenz oder andere vertraulichen Unternehmensdokumente. Das einzige Problem gestaltet sich dann, wenn die Konfiguration der Policies fehlerhaft durchgeführt wurde.

Es wird hier also auch stets ein sicherer Update-Mechanismus für neue Policies und Profile benötigt. SEAndroid wird bspw. bei KNOX von Samsung oder GATE von LG verwendet, um Apps gegenseitig zu kapseln.

4.7 Mobile Device Management (MDM)

Mobile Device Management-Anwendungen (MDM) greifen auf Schnittstellen, die das Betriebssystem bereitstellt, zu, um SMDs zentralisiert administrieren und konfigurieren zu können. Neben Funktionalitäten wie der Inventarisierung sowie der zentralen Fern-Konfiguration, -Wartung und -Überwachung der Geräte in Echtzeit ermöglicht das MDM auch die Überwachung sicherheitsrelevanter Konfigurationseinstellungen.

Im Bereich der sicherheitsrelevanten Konfigurationseinstellungen gewährleisten MDM-Lösungen insbesondere die einheitliche Sicherheitskonfiguration und helfen, die freie Konfigurier- und Erweiterbarkeit in gewissen Rahmenbedingungen einzuschränken. So ist beispielsweise einheitlich konfigurierbar, dass nur Passwörter mit einer definierten Stärke verwendet, die Daten bspw. lediglich verschlüsselt auf dem SMD abgelegt und unternehmenskritische Informationen nur über eine sichere VPN-Verbindung übertragen werden dürfen. Außerdem kann auch die Installation neuer Apps mittels White- und Blacklisting eingeschränkt werden. Über eine Geolokalisierung lassen sich außerdem entwendete oder verlorene mobile Geräte orten und die Inhalte ggfs. remote löschen. Zudem kann eine Selbstlöschung der Daten und des gesamten SMDs konfiguriert werden, sobald das System eine Manipulation des mobilen Gerätes durch die mehrmalige Fehleingabe des Kennwortes oder einen Jailbreak/Root-vorgang erkennt. Mobile Device Management-Systeme stellen somit wichtige Features zur Reduzierung der Risiken zur Verfügung. Als Beispiel für ein solches MDM sei hier das Produkt BizzTrust von der Firma Sirrix AG zu erwähnen.

5 Frühwarnung auf dem SMD

Alle bisher diskutierten Angriffsvektoren und Abwehrmaßnahmen basieren, sofern sie tatsächlich entdeckt werden können, auf dem Erkennungsprinzip. Anti-Malware-Software oder -Filter arbeiten erst dann zuverlässig, wenn diese mit echten Malwaresignaturen versehen worden sind, um auf deren Basis nach bekanntem Fehlverhalten Ausschau halten zu können. Dies hat zur Folge, dass zwar der Schutz vor bereits bekannten Bedrohungen besteht, diese Variante jedoch bei bis dato unbekannten Angriffen und Methoden in aller Regel versagt und dennoch die Daten, Kommunikationen und Geschäftsgeheimnisse bedroht sind. Erkannt werden kann also hierbei nur das, was bereits bekannt ist.

5.1 Automatische Analyse und Bewertung

Greift ein Angreifer in die Trickkiste und schafft es einen bis dato unbekannten Angriffsvektor zu verwenden, ist es schwierig bis unmöglich, mit normalen Hilfsmitteln etwas dagegen zu unternehmen und zu reagieren. Daher werden zusätzlich intelligente Systeme benötigt, welche in der Lage sein müssen, unbekannte Bedrohungen und Angriffe auf Basis von „Verhalten" der Malware sowie der Überwachung und Auswertung des Netzverkehrs innerhalb des Android-Betriebssystems zu erkennen.

Einen solchen Anomalieerkennungsansatz verfolgt das Forschungsprojekt SAiM (Schutz Androids durch intelligentes Monitoring), gefördert von dem Bundesministerium für Bildung und Forschung (BMBF). Hierbei wird auf die Erfahrung im Bereich Internet-Frühwarnung der beteiligten Partner zurückgegriffen, welche sich beim Schutz von größeren Netzwerken bereits bewährt hat. Die Entwicklung des SAiM-Prototypen wird auf Basis einer aktuellen Version des OpenSource-Betriebssystems Android durchgeführt. Der Prototyp erlaubt ein mobiles Gerätemanagement, was die zentralisierte Verwaltung von Mobilgeräten durch die jeweiligen Administratoren erlaubt. Diese behalten stets den Überblick über potentiell schädliche Aktivitäten und können so zeitnah Gegenmaßnahmen einleiten, falls nötig. Die gesamte Planung und Umsetzung wird dabei in Deutschland durchgeführt und erfüllt die strengen deutschen Datenschutzbestimmungen.

5.2 Usability und Praxistauglichkeit

Ein wichtiger Kern dieser Sicherheitslösung soll ein selbstlernendes System sein, das sowohl bösartige Apps als auch Netzwerkangriffen erkennt und meldet. Hierbei werden verschiedene Netzwerk- und Betriebssystemdaten zur Laufzeit gemessen und mit Methoden der Künstlichen Intelligenz ausgewertet. Es sollen also neuartige Bedrohungen detektiert werden, zu denen es noch keine Angriffssignaturen gibt. Zudem soll es auf freiwilliger Basis eine Möglichkeit geben, anonymisierte Messdaten von vielen SMDs an einer zentralisierten Stelle auszuwerten, um noch besser Bedrohungen zu erkennen und bspw. Verbreitungen zu visualisieren. Gleichzeitig sollen die verwendeten Algorithmen neue gute Zustände mitlernen, um die Erkennungsrate an Bedrohungen zu erhöhen.

Ein wichtiges Kernthema ist im Hinblick auf die Architektur die praktische Umsetzung der Prototypen in Form einer App, basierend auf einem eigens hierfür entwickelten Framework. Hierzu werden notwendigerweise zahlreiche anonymisierte Messwerte innerhalb des Gerätes in Echtzeit gespeichert und auf Anomalien hin überprüft. Wenn optional auch Daten an einen zentralisierten Server zur noch besseren Analyse gesendet werden, bekommt der Anwender bei erkannten Bedrohungen direktes Feedback auf sein SMD.

6 Fazit

Der Mobilbereich und damit die SMD-Verwendungen werden auch in der Zukunft weiter steigen. Genauso wird sich das Angebot der Apps weiter vergrößern, aber damit auch die Risiken bei deren Benutzung. Es ist noch ein weiter Weg, eine vertrauenswürdige Nutzung bei SMDs zu gewährleisten. Als Privatanwender sollte ein Rooten des Geräts auf jeden Fall vermieden werden, da anschließend aufgrund der nicht mehr greifenden Betriebssystem-Sicherheitsmechanismen mehr Bedrohungen ermöglicht werden. Üblicherweise sind auch immer kostenpflichtige Apps den kostenlosen, die sich aus Werbung finanzieren, vorzuziehen, da bspw. Werbeeinblendungen auch immer aktuelle Dokumente auf dem SMD ausspähen können. Natürlich sollte auch bei bezahlten Apps die Berechtigungen geprüft werden, ob es z.B. wirklich nötig ist, für eine Taschenlampen-App ständig GPS-Koordinaten zu versenden. Aktuelle Datenschutzkonzepte vieler Apps

sind rechtlich bedenklich, und die Einhaltung der Hersteller kann in dem riesigen Umfang nicht hinreichend geprüft werden. Es gilt also auch hier das Gebot der Datensparsamkeit.

Gerade Unternehmen sollten ihren Mitarbeitern für die erhöhte Produktivität SMDs, aber mit den nötigen Schutzfunktionen, zur Verfügung stellen. Hierbei gilt: Wenn das Unternehmen das SMD bezahlt und verwaltet, kann ein sehr viel höherer Schutz gewährleistet werden. Um die Akzeptanz bei den Mitarbeitern zu steigern sollte auch eine Privatnutzung eingeräumt werden, da es hierfür ausreichende Schutzkonzepte gibt. Wird mit sehr sensiblen Daten hantiert und auch in besonders kritischen Bereichen, reichen bisherige Schutzmechanismen nicht aus. Hier werden moderne Konzepte benötigt, wie sie bspw. das Forschungsprojekt SAiM mit intelligenter Anomalieerkennung verfolgt.

Die eingesetzten Schutzmechanismen müssen immer auf die zu schützenden Werte abgestimmt werden. Ein 100%igen Schutz kann insgesamt zwar nicht gewährleistet werden, aber es kann dem Angreifer extrem schwer gemacht werden, sodass dieser aufgrund des hohen Aufwands von seinem kriminellen Vorhaben Abstand nimmt. Des Weiteren sollte jeder Anwender seinen gesunden Menschenverstand einsetzen. Alle Schutzmechanismen schützen das SMD, aber nicht den unerfahrenen Anwender vor sich selbst.

Literatur

BITKOM: Jeder Vierte nutzt durchschnittlich 23 Apps; http://www.go2android.de/bitkom-jeder-vierte-nutzt-durchschnittlich-23-apps/

Smartphone Honey Stick Project; http://www.symantec.com/content/en/us/about/presskits/b-symantec-smartphone-honey-stick-project.en-us.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2012Mar_worldwide_honeystick

Android: 1,5 Millionen Aktivierungen täglich, Tendenz steigend; http://www.androidnext.de/news/android-15-millionen-aktivierungen-taeglich-tendenz-steigend/

Projekt SAiM; https://www.internet-sicherheit.de/SAiM

Zahlen zu Google Play, Google: Statistiken über Android, Play Store & Nexus 7 – 50 Mrd. Downloads; http://www.googlewatchblog.de/2013/07/google-statistiken-android-play/